



**Promoting Intellectual
Property Rights in the
ASEAN Region**

Session 7: Best Practices on Investigative Techniques and Intelligence Gathering in relation to Online IPR Infringement Cases

Erling Vestergaard, Manila, 24-25 April 2019



Funded by the European Union



This Project is funded by the European Union and implemented by the European Union Intellectual Property Office (EUIPO)

Index

- **Challenges for Online Investigation**
- **Electronic Evidence**
- **Hardware and Software Requirements**
- **Open Source Intelligence (OSINT)**
- **Cooperation with Internet Intermediaries**
- **Data Interception and Cross border Data Exchange**
- **Search and Seizure**
- **Search and Seizure: Romanian IPTV Example**
- **Anti-Forensic Strategies**
- **Darknet Marketplace Investigation**

Challenges for Online Investigation

Challenges for Online Investigation

Cyberspace

"A graphic representation of data abstracted from the banks of every computer in the human system."

William Gibson: Neuromancer (1984)

Challenges for Online Investigation

- ☐ Anonymization
- ☐ Scale and proximity
- ☐ Jurisdictional limitations
- ☐ Technical capability of investigators
- ☐ New criminal structures unique for online environment: Swarms and Hubs
- ☐ Criminal patterns and modus operandi
- ☐ Anti-forensic strategies (...more about that later)

Cyberspace

"A graphic representation of data abstracted from the banks of every computer in the human system."

William Gibson: Neuromancer (1984)

Challenges for Online Investigation

- ☐ Anonymization
- ☐ Scale and proximity
- ☐ Jurisdictional limitations
- ☐ Tech
- ☐ New
- ☐ Hub
- ☐ Crim
- ☐ Anti

Cyberspace

"A graphic representation of data abstracted from the banks of every computer in the human system."

William Gibson: Neuromancer (1984)

Susan Brenner 'Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?', 30 Rutgers Computer & Tech. L.J. 1, 104 (2004)

"... cybercrime differs in several fundamental aspects from real-world crime, the type of crime which our existing model of law enforcement was developed to address. As a result, the traditional model is not an effective means of dealing with cybercrime."

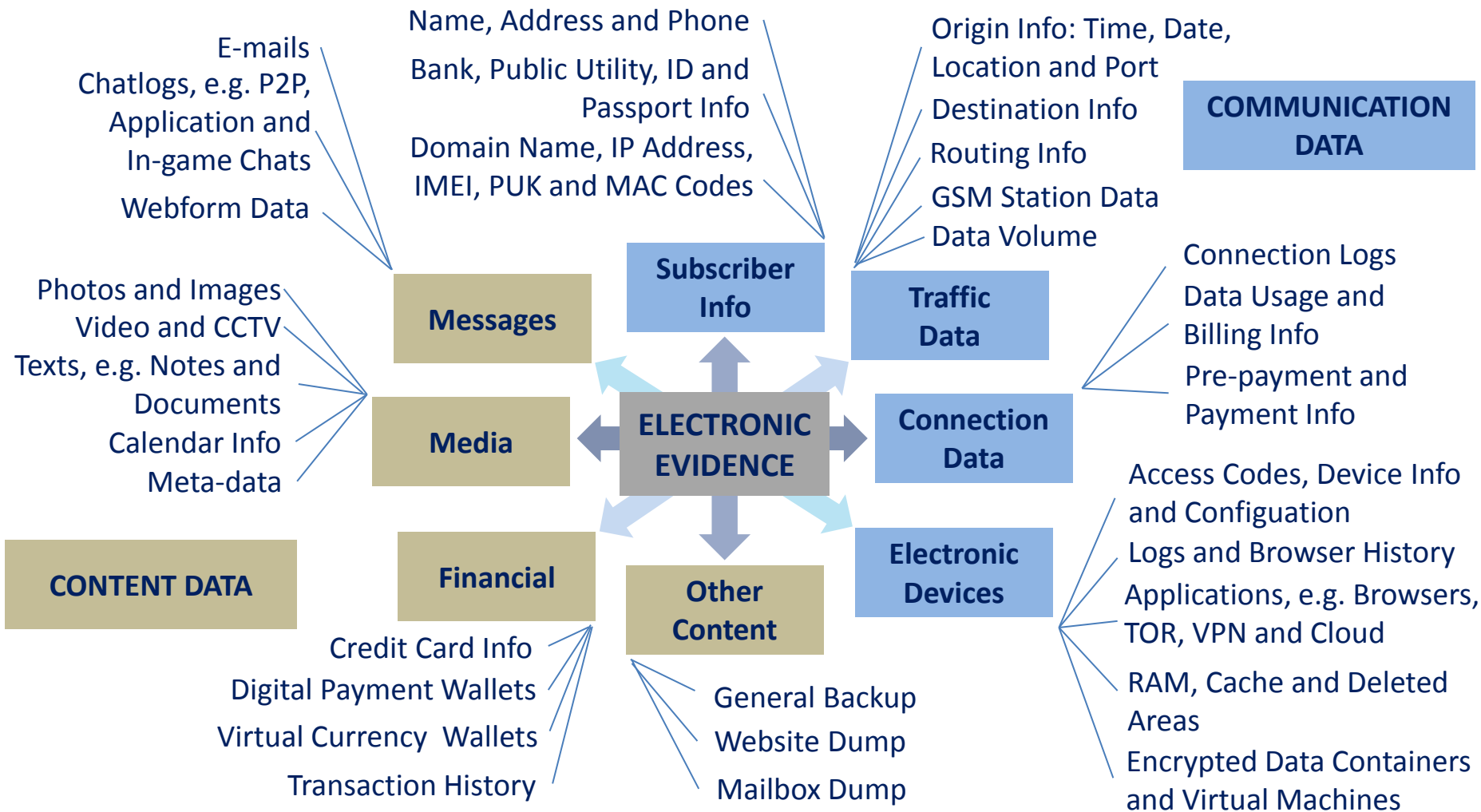
s and

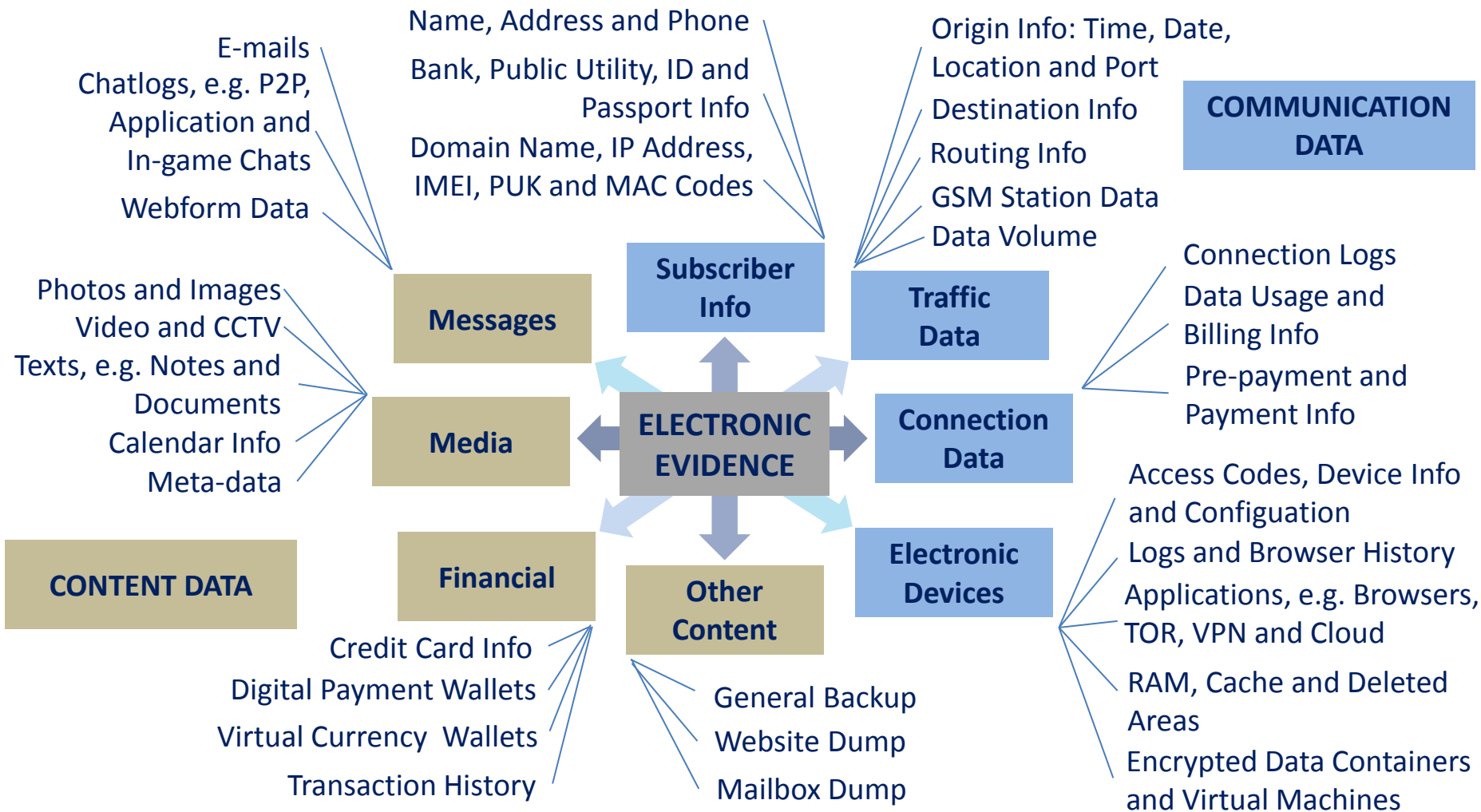
Electronic Evidence

Electronic Evidence

- ☐ Electronic Data Processing
 - Quantum Mechanics
 - Mathematics
- ☐ Computer Devices
- ☐ Storage Media
- ☐ Computer Programs
- ☐ Data (metadata, content data)



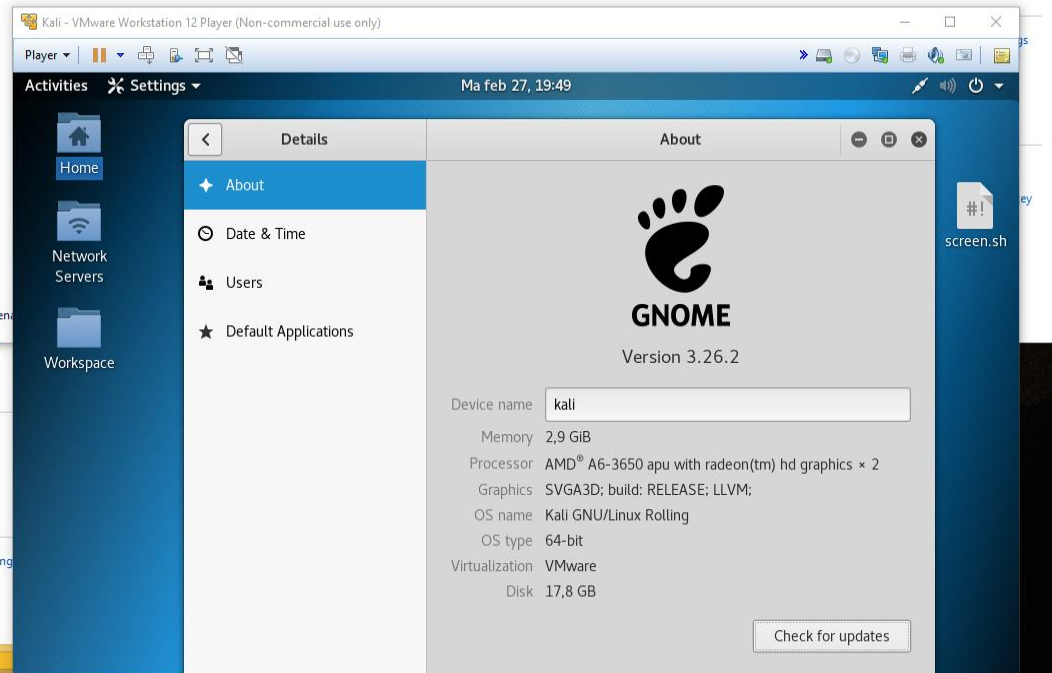
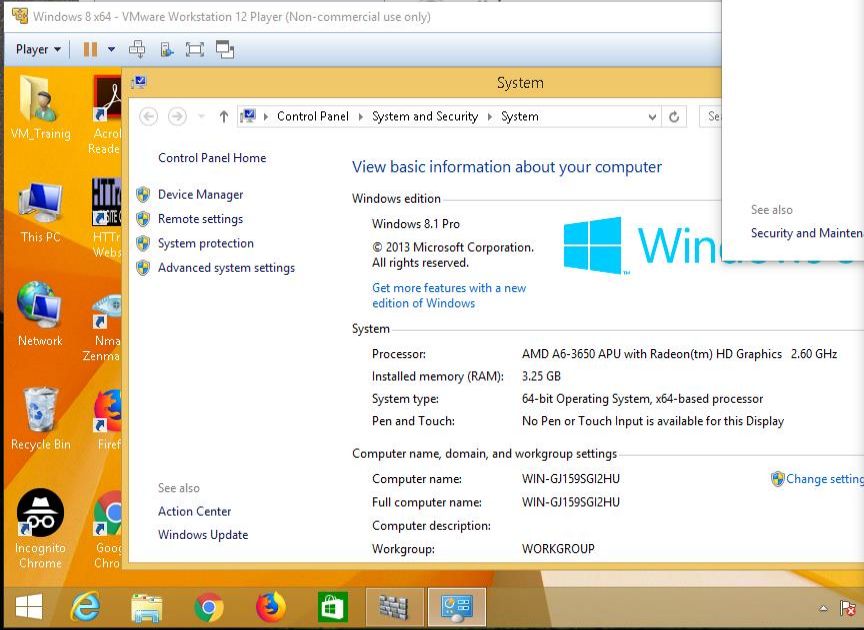
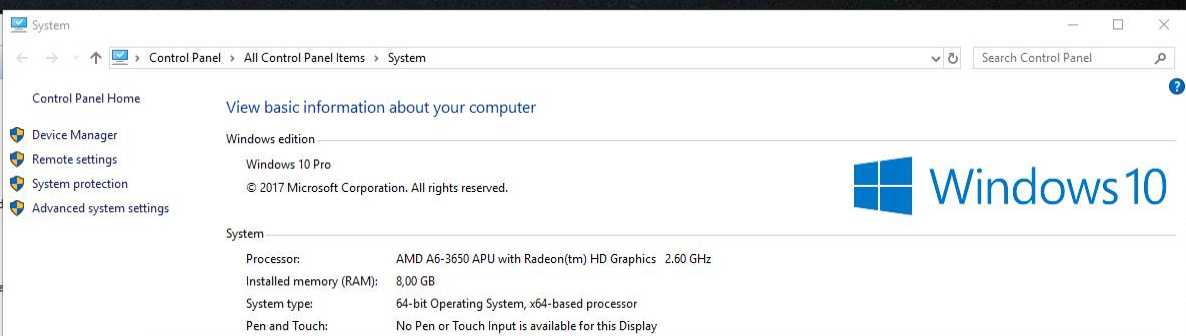
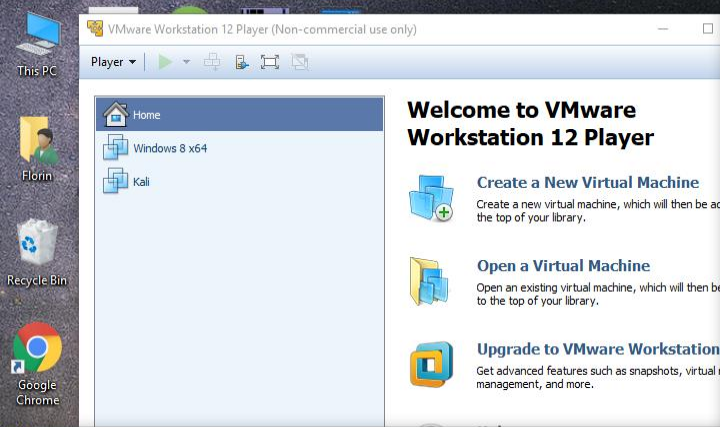




Hardware and Software Requirements

Hardware and Software Requirements

- ☐ Isolated stand alone equipment
- ☐ Secure backup
- ☐ Up to date security software
- ☐ Undercover identities – Gmail, Outlook, Yahoo, Facebook, etc.
- ☐ Virtual Private Network (VPN), Virtual Private Machine (VPM)

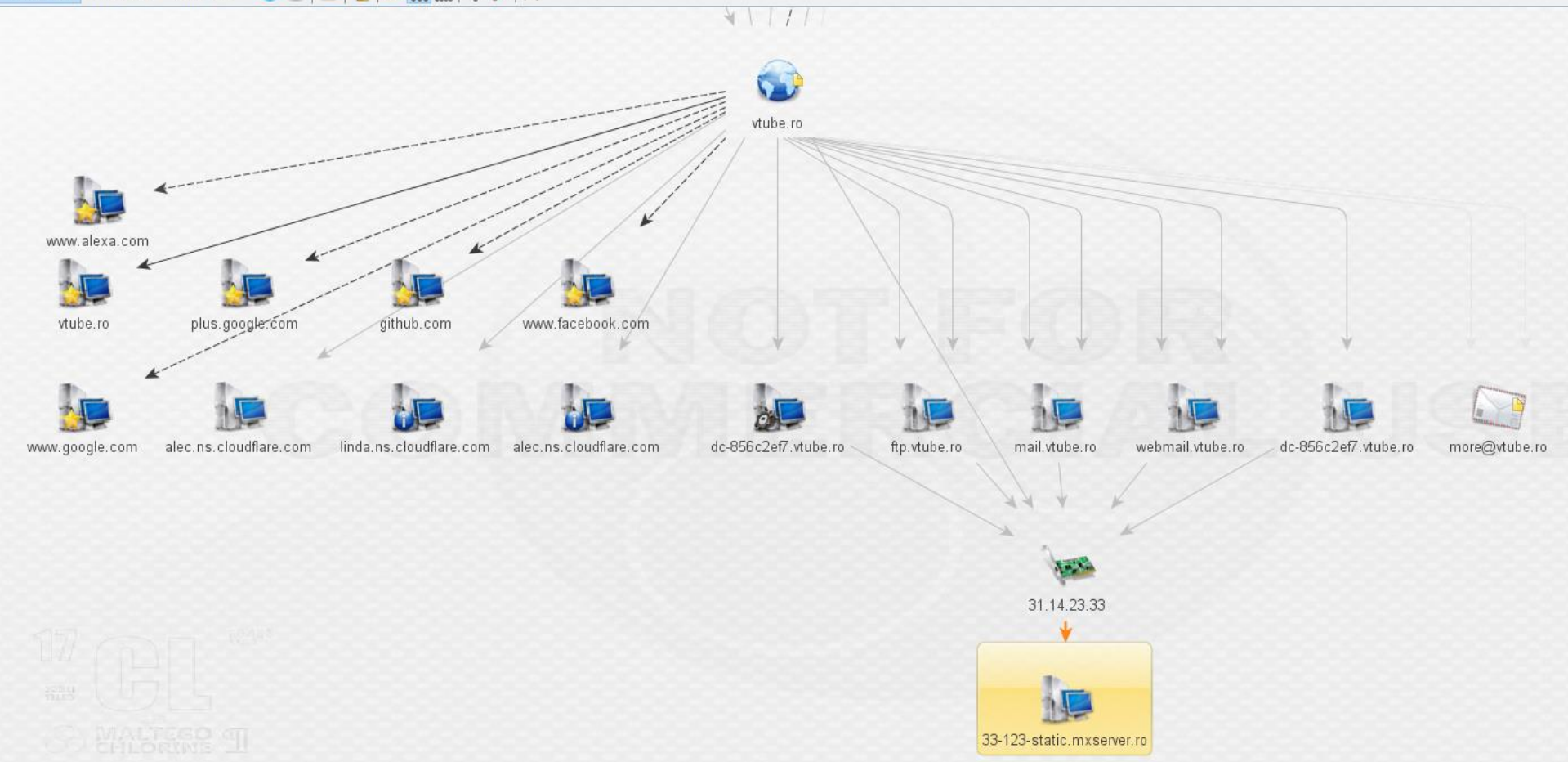


Hardware and Software Requirements

- ☐ Browser setup
 - All browsers have special strengths = utilise all
 - Clear all browsing data at the beginning of an investigation (cookies, site plugin data, app data, cached images, etc.)
 - Use Incognito – Private – InPrivate mode
- ☐ Website copier (e.g. HTTrack)

Hardware and Software Requirements

- ❑ Determine relationships and real world links (e.g. Maltego)
 - Simple verification of email addresses, search blogs for tags and phrases, identify incoming links for websites, extract metadata from files from target domains
 - Enumerate network and domain information like domain names, WHOIS information (if available), DNS names, IP blocks, IP addresses etc.
 - Correlate email addresses, web sites, phone numbers, social media groups, companies and organizations



Personal

- Registrant**
Domain Registrant
- Alias**
An alias for a person
- Document**
A document on the Internet
- Email Address**
An email mailbox to which email messages may be delivered
- Image**
A visual representation of something
- Person**
Entity representing a human
- Phone Number**
A telephone number
- Phrase**
Any text or part thereof
- Skype ID**
Skype UserID

Social Network

- Facebook Object**
Facebook Object
- Affiliation - LinkedIn - Person**
This is a LinkedIn Affiliation entity
- Affiliation - LinkedIn - Company**
This is a LinkedIn Company Profile entity
- LinkedIn - Update**
LinkedIn - Update
- Twit**
Twit entity
- Affiliation - Facebook**
Membership of the Facebook social network
- Affiliation - Twitter**
Membership of Twitter
- Hashtag**
Twitter hashtag

Devices

Groups

- Registrar**
Domain Registrar
- Organization**
A social group which distributes tasks for a collective goal

Infrastructure

- AS**
An internet Autonomous System (AS)
- DNS Name**
Domain Name System server name
- Domain**
An internet domain
- IPv4 Address**
An IP version 4 address
- MX Record**
A DNS mail exchange record
- NS Record**
A DNS name server record
- Netblock**
An internet Autonomous System (AS)
- URL**
An internet Uniform Resource Locator (URL)
- UniqueIdentifier**
Uniquely identifier for a website service.
- Website**
An internet website

Locations

- Circular Area**
A circular area somewhere on Earth
- GPS Coordinate**
A location on a World Geodetic System coordinate frame
- Location**
A location on Mother Earth

Detail View

Domain
maltego.Domain
online-film.hu

- Relationships

- Incoming

info@online-film.hu +36-70-429-2051	János Tóth
--	------------

- Outgoing

mail.online-film.hu www.online-film.hu www.online-film.hu postmaster@online-film.hu	ftp.online-film.hu mail.online-film.hu ns1.w3host.hu www.online-film.hu
--	--

- Notes

E2:No email in whois
E2:No entities in whois
E2:No email in whois

- Generator detail

Source	info@online-film.hu	(Email Address)
Transform	To Domain [DNS]	
Gen. date	2016-08-15 14:32:16.93 +0300	

Property View

Properties

Type	Domain
Domain Name	online-film.hu
WHOIS Info	domain: online-film.hurecord crea...
Graph info	
Weight	50
Incoming	3
Outgoing	8
Bookmark	★

Hardware and Software Requirements

- ☐ Secure handling of electronic evidence
- ☐ Automated backup
- ☐ Reliable digital forensic tools (e.g. Encase)
- ☐ Replicable analyses results (Turing completeness)

Open Source Intelligence (OSINT)

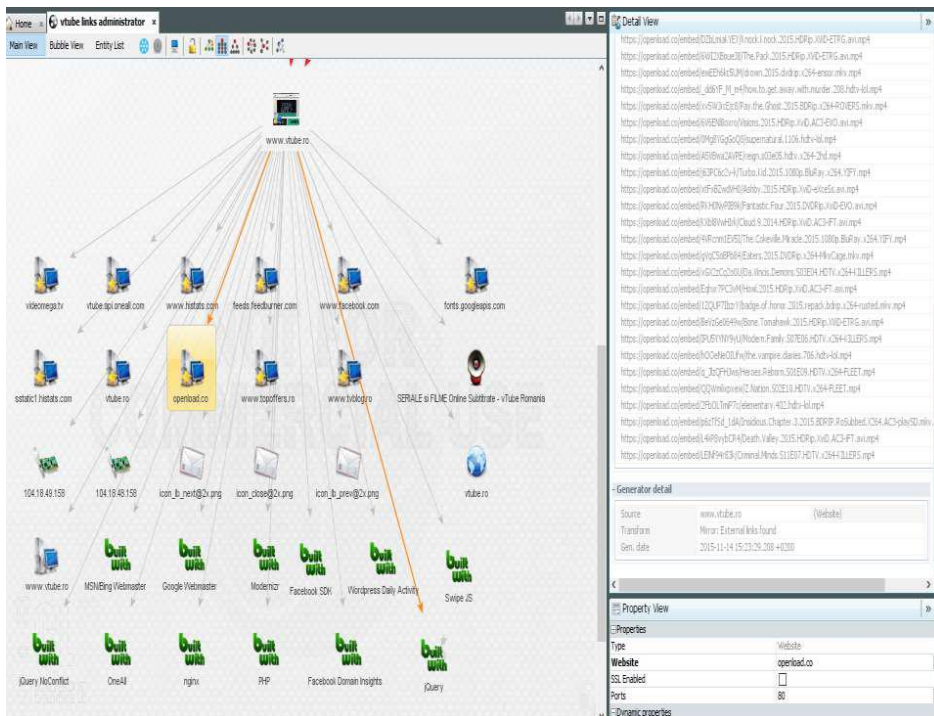
Open Source Intelligence (OSINT)

- ❑ OSINT: Diverse forms of intelligence gathering and analysis
- ❑ OSINT tools: Kali Linux, Python Scripts, Maltego, OSINTUX etc
- ❑ Identifying relevant and reliable publicly available data sources



Open Source Intelligence (OSINT)

- ❑ Enumerate network info to determine relationships and real world links
- ❑ Virtual currency analysis



Cooperation with Internet Intermediaries

Cooperation with Internet Intermediaries



Transparency Report Help Center

Legal process for user data requests FAQs

Requests from outside the United States

[How does Google respond to requests from government agencies outside the United States?](#) ^

On a voluntary basis, we may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, Google's policies and the law of the requesting country.

Cooperation with Internet Intermediaries

facebook

Law Enforcement Online Requests



Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent or emergency responder who is authorized to gather evidence in connection with an official investigation or in order to investigate an emergency involving the danger of serious physical injury or death, you may request records from Facebook through this system.

☐ I am an authorized law enforcement agent or government employee investigating an emergency, and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Law Enforcement Guidelines](#).

Cooperation with Internet Intermediaries

coinbase

Products ▾

Help

Charts

Sign In

Sign Up

LEGAL

[USER AGREEMENT](#)

[PRIVACY POLICY](#)

[COOKIE POLICY](#)

[LICENSES](#)

[INSURANCE](#)

[MARKET DATA](#)

[FAQ](#)

- We may share your information with any third parties where required to do so by applicable law or any court or other authority to which we are subject in any jurisdiction; or we believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity or to investigate violations of the CB User Agreement and any other applicable policies.^a

Cooperation with Internet Intermediaries

Who may *voluntarily* provides evidence?

- ☐ Apple: <http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf> ☐
- ☐ Dropbox: <https://www.dropbox.com/transparency>
- ☐ Facebook: <https://www.facebook.com/safety/groups/law/guidelines>
- ☐ Google:
<https://www.google.com/transparencyreport/userdatarequests/legalprocess/>
- ☐ Instagram: <https://help.instagram.com/494561080557017/>
- ☐ LinkedIn: <https://www.linkedin.com/help/linkedin/answer/16880?lang=en>
- ☐ Snapchat: https://www.snapchat.com/static_files/lawenforcement.pdf
- ☐ Twitter: <https://support.twitter.com/articles/41949#>
- ☐ And others

Cooperation with Internet Intermediaries

What evidence may be provided? (1) Basic Subscriber Information, e.g.

- ☐ Account or login name
- ☐ Name, physical address, telephone number and email address
- ☐ IP address used to register the account or otherwise initiate service, and used to log into the account
- ☐ Session times, dates and duration
- ☐ Any other information pertaining to the identity of the subscriber, including billing information

Cooperation with Internet Intermediaries

What evidence may be provided? (2) Transactional Information, e.g.

- ☐ Connection information for other systems to which the user connected via the email account/web host account, incl. connection destination or source of connection, connection time and date, disconnect time and date, method of connection to system (e.g. telnet, ftp, http), data transfer volume (e.g. bytes) and any other relevant routing information
- ☐ Source of destination of any electronic mail messages sent from or received by the account, and the date, time, and length of the message
- ☐ Information pertaining to any image(s) or other documents uploaded to the account/website, including the dates and times of upload, and the size of the files
- ☐ Name and other identifying details of individuals that accessed a specific image/file/web page in a specified period of time, on a specific date

Cooperation with Internet Intermediaries

What about Content Data?

- ☐ Content data will normally *not* be voluntarily shared
- ☐ Some internet intermediaries *might* provide voluntary data retention ('freezing') of content data
- ☐ The data can then be obtained through MLA if legal requirements are met (e.g. in the US, 'probable cause')

Data Interception and Cross border Data Exchange

Data Interception and Cross border Data Exchange

- ☐ Cybercrime convention, 2001, 64 countries ratified (incl. Philippines)
- ☐ G7 24/7 network (70+ countries), single points of contact
- ☐ US Cloud Act and EU E-evidence proposal
- ☐ Data retention order ('freezing')
- ☐ Production order
- ☐ Data interception
- ☐ Alternative cross border data access?
- ☐ Government hacking?



Search and Seizure

Search and Seizure

- ☐ **Secure** the Area and *'Hands from Computers'* and *'Keep Computers Switched On'*
- ☐ **Document** Crime Scene and Photograph Screens
- ☐ Identify **All** Devices
- ☐ Complete Data **Mirrors**
- ☐ Securing **Temporary** Data (Caches and Logs)
- ☐ Different Crimes have different **Technical** Requirements



Kuala Lumpur Raid Against
Illegal IPTV Data Centre

Search and Seizure

And Secure Physical Evidence:

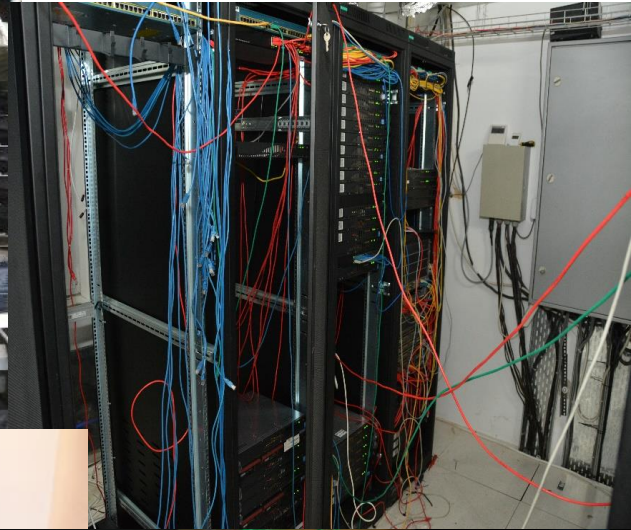
- ☐ Diaries and Notebooks
- ☐ Passwords
- ☐ Pictures
- ☐ Drawings
- ☐ Print Outs
- ☐ Business Plans
- ☐ Garbage
- ☐ Virtual Currency Account/Wallet Recovery Codes



Kuala Lumpur Raid Against
Illegal IPTV Data Centre

Search and Seizure: Romanian IPTV Example





Search and Seizure: Romanian IPTV Example

Video


Anti-Forensic Strategies

Anti-Forensic Strategies

- ☐ **Awareness** and Sharing of Law Enforcement Strategies
- ☐ Operational (traditional) **Protective** Security Measures
- ☐ **Flushable** Media to Install Malware
- ☐ Media Wiping and Memory **Deletion**
- ☐ **Anonymization**, Encryption, Virtual Machine and Virtual Machine in Virtual Machine
- ☐ File Signature **Altercation**
- ☐ IT Forensic Program **Detection**
- ☐ IT Investigator **Human Engineering** Attack
- ☐ IT Forensic Resource **Waste**
- ☐ Metadata **Manipulation** and Misleading Evidence
- ☐ **Rootkits** and Slack (Empty) Space Manipulation used to Install Malware
- ☐ **Homographic** Attack (Misleading Letters or Words)
- ☐ **Stenography** (Hidden Information)
- ☐ Packers/**Binders** (Change of File Structure to Bypass Detection)

Darknet Marketplace Investigation

Darknet Marketplace Investigation


Silk Road
 anonymous market

messages 0 | orders 0 | account \$0.0000 \$0.00













a few words from the Dread Pirate Roberts

Hi, cirrus
 about

Search

Shop by Category

Drugs 13,810
 Cannabis 2,934
 Dissociatives 199
 Ecstasy 1,274
 Intoxicants 75
 Opioids 367
 Other 82
 Precursors 62
 Prescription 4,659
 Psychedelics 1,754
 Stimulants 1,634
 Tobacco 219
 Apparel 767
 Art 15
 Books 1,322
 Collectibles 27
 Computer equipment 107
 Custom Orders 86
 Digital goods 886
 Drug paraphernalia 512
 Electronics 234
 Erotica 584
 Fireworks 35
 Food 10
 Forgeries 152
 Hardware 35
 Home & Garden 27
 Jewelry 104
 Lab Supplies 29
 Lotteries & games 165
 Medical 60
 Money 258
 Musical instruments 6
 Packaging 95
 Services 168
 Sporting goods 4
 Tickets 4
 Writing 8

 Boldabol 200 (B. Dragon), 10ml, 200mg/ml \$66.11	 PIRACETAM 1200mg 100x1200mg (nootropil) \$92.64	 25X LSD BLOTTER \$421.19
 7 grams of PURE MDMA Moonrocks. \$378.58	 100x Green Android™ (The New Mortal Kombi™) \$547.65	 2mg Xanax Bars from Walgreens \$5.42
 10.0g MDA - Reagent Tested \$550.00	 HYDRO BUDS 2G \$40.00	 SCIROXX - Nandrodex 300mg/ml 10ml USA ONLY \$114.21
 10g Amnesia Haze \$194.77	 4 Orange sunshine 300ug \$90.49	 1/4 Bubba Kush \$90.20

From the forum

- Buyer ratings discussion
- Feedback system changes
- HOW TO: Run your own relay and help the Tor network!
- Ask a drug expert physician about drugs and health
- Winning the war on drugs
- New display currencies
- Try Tails for a more secure OS

Favorite vendors

- Dread Pirate Roberts 5.0 - remove
- Libertas 1.0 - remove
- Inigo 0.0 - remove

GOVERNMENT EXHIBIT
132
14 Cr. 88 (CRP)

@1 = \$133.74

community forums | wiki | support

Darknet Marketplace Investigation

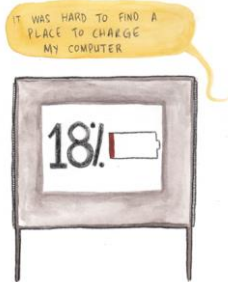
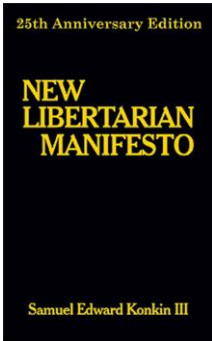


First Darknet Market Takedown: The Silk Road, October 2013

- Main tool for investigation: Infiltration
- Stylometry
- Exploit of technical faults on website



'Dread Pirate Roberts

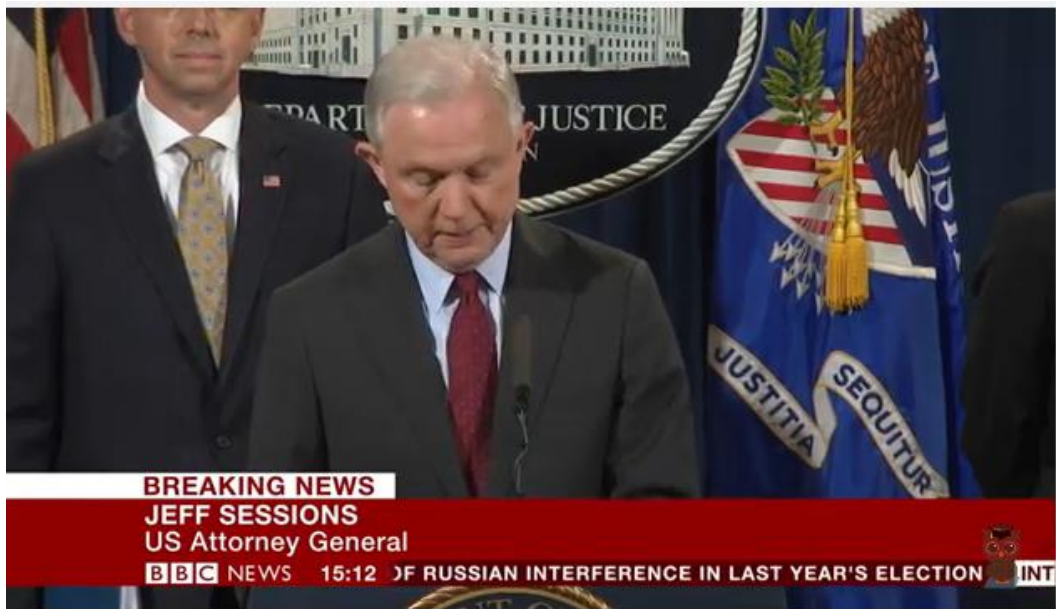


Darknet Marketplace Investigation



- First Major Darknet Market
Coordinated Action:
Operation 'Onymous', November
2014
- Takedown of 410 TOR 'Hidden Services'
 - Main tool for investigation: TOR nodes control and DDOS attack

Darknet Marketplace Investigation



- Takedown of Alpha Bay and Hansa Markets, July 2017
- Exploit of test website fault
 - Good cooperation with private sector
 - Infiltration
 - Placement of 'beacons' on vendor computers
 - Expedient international cooperation



Promoting Intellectual
Property Rights in the
ASEAN Region

THANK YOU

erling.vestergaard@euipo.europa.eu



Funded by the European Union



This Project is funded by the European Union and implemented by the European Union Intellectual Property Office (EUIPO)